Amendments to the Claims

The listing of claims below will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A computer implemented method for securing a file, the method comprising:

determining whether the file stored in a file system and being accessed is secured;

if the file is determined to be secured, activating a cipher module and loading the file from the file system through the cipher module into an application; and

if the file is determined to be non-secured, loading the file from the file system into the application without activating the cipher ~~module.~~ module, wherein the file includes a header having a file key, the file key is encrypted with a user key, and the user key is different from the file key.

2. (Previously Presented) The method of Claim 1, wherein the cipher module, once activated, operates within an operating system.

3. (Canceled)

4. (Currently Amended) The method of Claim 1, wherein the file further includes ~~a header and~~ an encrypted ~~portion,~~ portion and the header ~~including~~ includes or ~~pointing~~ points to security information including [[a]] the file key used to decrypt the encrypted portion.

5. (Currently Amended) [[The]] A computer implemented method ~~of Claim 4, wherein the determining whether the file stored in the file system and being accessed is secured comprises~~ for securing a file, the method comprising:

determining if the file stored in [[the]] a file system and being accessed includes ~~the header~~ a header, wherein existence of the header indicates that the file is secured;

if the file is determined to be secured, activating a cipher module and loading the file from the file system through the cipher module into an application; and

if the file is determined to be non-secured, loading the file from the file system into the application without activating the cipher module.

6. (Currently Amended) [[The]] A computer implemented method ~~of Claim 4,~~ for securing a file, the method comprising:

~~wherein the header further includes a flag indicating that the file stored in the file system and being accessed is secured, and~~

~~wherein the determining of whether the file stored in the file system and being accessed is secured comprises~~

determining if the file stored in a file system and being accessed has ~~the flag.~~ a flag, wherein existence of the flag indicates that the file is secured;

if the file is determined to be secured, activating a cipher module and loading the file from the file system through the cipher module into an application; and

if the file is determined to be non-secured, loading the file from the file system into the application without activating the cipher module.

7. (Previously Presented) The method of Claim 4, wherein the loading the file from the file system through the cipher module into the application comprises:

retrieving the file key;

decrypting the encrypted portion with the file key in the cipher module; and

sending the file in clear mode to the application.

8. (Currently Amended) The method of Claim 7, ~~wherein the security information including the file key is encrypted with a user key, and~~ wherein the retrieving the file key comprises:

obtaining the user ~~key associated with a user requesting an access to the file;~~ key; and

decrypting [[the]] security information including the file key with the user key to retrieve the file key.

9. (Currently Amended) [[The]] A computer implemented method ~~of Claim 8,~~ for securing a file, the method comprising:

determining whether the file stored in a file system and being accessed is secured, wherein the file includes a header and an encrypted portion, the header including or pointing to security information including a file key used to decrypt the encrypted portion, wherein the security information including the file key is encrypted with a user key, and wherein the security information further includes access rules to control how and by whom the file is to be ~~accessed.~~ accessed;

if the file is determined to be secured, activating a cipher module, loading the file from the file system through the cipher module into an application, retrieving the file key, obtaining the user key, decrypting the security information with the user key to retrieve the

file key, and decrypting the encrypted portion with the file key in the cipher module, and sending the file in clear mode to the application; and

if the file is determined to be non-secured, loading the file from the file system into the application without activating the cipher module.

10. (Currently Amended) The method of Claim 9, wherein the loading the file from the file system through the cipher module into the application only happens if an access privilege ~~of the user~~ is within permissions granted by the access rules.

11. (Previously Presented) A computer implemented method for securing a file, the method comprising:

maintaining a file key in a temporary memory space;

encrypting the file with the file key in a cipher module to produce an encrypted portion;

preparing security information for the encrypted portion, the security information being encrypted with a user key and including the file key and access rules to control access to the encrypted portion, wherein the access rules in the security information comprise user information identifying who has access to the encrypted portion and how the encrypted portion is to be accessed; and

attaching the security information to the encrypted portion.

12. (Previously Presented) The method of Claim 11, further comprising deleting the file key from the temporary memory space when the attaching the security information to the encrypted portion is complete.

13. (Currently Amended) The method of Claim 11, wherein the encrypting the file with the file key, the preparing the security information, and the attaching the security information happen whenever the file is caused to be ~~stored in a storage space.~~ stored.

14. (Previously Presented) The method of Claim 11, wherein the encrypting the file with the file key, the preparing the security information, and the attaching the security information happen upon receiving an instruction from an application or an operating system supporting the application.

15. (Canceled)

16. (Currently Amended) The method of Claim 14, wherein the instruction is one of (i) Save, (ii) Close [[and]] or (iii) Exit, all provided in the application.

17. (Previously Presented) The method of Claim 14, wherein the instruction is generated from an automatic operation of saving the file being opened into a storage space, the automatic operation being triggered by the application itself or the operating system.

18. (Previously Presented) The method of Claim 11, wherein the user key is associated with a member selected from a group consisting of a user, a device, a software module, and a group of users.

19. (Canceled)

20. (Currently Amended) A computer implemented method for providing access control to a file, the method comprising:

forwarding a request to access the file to a file system manager in an operating system;

activating a document securing module by the file system manager to determine whether the file stored in a file system driver and being accessed is ~~secured;~~ secured, wherein the file includes a header having a file key, the file key is encrypted with a user key, and the user key is different from the file key;

activating a cipher module if the file is determined to be secured; and

loading the file from the file system driver through the cipher module into an application.

21. (Currently Amended) The method of Claim 20, further comprising:

retrieving security information from the file if the file is determined to be secured, the security information including [[a]] the file key and access rules; and

obtaining an access privilege ~~of a user~~ requesting to access the file.

22. (Previously Presented) The method of Claim 21, wherein the activating the cipher module proceeds successfully when the access privilege is within permissions granted by the access rules.

23. (Previously Presented) The method of Claim 22, wherein the activating the cipher module comprises decrypting an encrypted portion of the file with the file key.

24. (Currently Amended) A ~~computer readable storage~~ tangible computer-readable medium having ~~computer program code recorded~~ stored thereon, ~~that when executed by a processor, causes the processor to access a file by a method,~~ computer-executable instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

determining whether the file stored in a file system and being accessed is secured;

if the file is determined to be secured,

activating a cipher module; and

loading the file from the file system through the cipher module into ~~the~~ an application; and

if the file is determined to be non-secured,

loading the file from the file system into the application without activating the cipher ~~module.~~ module;

wherein the file includes a header having a file key, the file key is encrypted with a user key, and the user key is different from the file key.

25. (Currently Amended) The ~~computer-readable storage~~ tangible computer-readable medium of Claim 24, wherein the file further includes ~~a header and~~ an encrypted ~~portion,~~ portion and the header ~~including~~ includes or ~~pointing~~ points to security information including [[a]] the file key used to decrypt the encrypted portion.

26. (Currently Amended) ~~The computer readable storage~~ A tangible computer-readable medium ~~of Claim 25, wherein the determining whether the file stored in the file system and~~

~~being accessed is secured comprises~~ having stored thereon, computer-executable instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

determining if the file stored in [[the]] a file system and being accessed includes ~~the header.~~ a header, wherein existence of the header indicates that the file is secured;

if the file is determined to be secured,

activating a cipher module; and

loading the file from the file system through the cipher module into the application; and

if the file is determined to be non-secured,

loading the file from the file system into the application without activating the cipher module.

27. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim [[25,]] 26, wherein the loading the file from the file system driver through the cipher module into the application comprises:

retrieving the file key;

decrypting [[the]] an encrypted portion with the file key in the cipher module; and

sending the file in clear mode to the application.

28. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 27, ~~wherein the security information including the file key is encrypted with a user key, and~~ wherein the retrieving the file key comprises:

obtaining the user ~~key associated with a user requesting an access to the file;~~ key; and

decrypting [[the]] security information including the file key with the user key to retrieve the file key.

29. (Currently Amended) ~~The computer-readable storage~~ A tangible computer-readable medium ~~of Claim 28,~~ having stored thereon, computer-executable instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

determining whether the file stored in a file system and being accessed is secured, wherein the file includes a header and an encrypted portion, the header including or pointing to security information including a file key used to decrypt the encrypted portion, wherein the security information including the file key is encrypted with a user key, and wherein the security information further includes access rules of how and by whom the file is to be ~~accessed.~~ accessed;

if the file is determined to be secured,

activating a cipher module; and

loading the file from the file system through the cipher module into the application;

retrieving the file key;

obtaining the user key;

decrypting the security information with the user key to retrieve the file key;

decrypting the encrypted portion with the file key in the cipher module; and

sending the file in clear mode to the application; and

if the file is determined to be non-secured,

loading the file from the file system into the application without activating the cipher module.

30. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 29, wherein the loading the file from the file system through the cipher module into the application proceeds only when an access privilege ~~of the user~~ is within permissions granted by the access rules.

31. (Currently Amended) A ~~computer readable storage~~ tangible computer-readable medium having ~~computer program code recorded~~ stored thereon, computer-executable instructions that ~~when~~ if executed by a ~~processor, causes~~ computing device, cause the ~~processor~~ computing device to ~~secure a file by a method,~~ perform a method comprising:

maintaining a file key in a temporary memory space;

encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and the cipher module operates transparently as far as a user executing the application is concerned; and

storing, in a storage space, a secured file including the encrypted file and a header, wherein the header includes or points to security information including the file key, wherein the security information further includes access rules of how and by whom the file is to be accessed.

32. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 31, further comprising deleting the file key from the temporary memory space when the application ~~is caused to close~~ closes the file.

33. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 31, wherein the encrypting the file with the file key happens whenever the file is caused to be ~~stored in the storage space.~~ stored.

34. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 31, wherein the encrypting the file with the file key happens upon receiving an instruction from the application or an operating system supporting the application.

35. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 34, wherein the instruction is one of (i) Save, (ii) Close [[and]] or (iii) Exit, all provided in the application.

36. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 34, wherein the instruction is generated from an automatic operation of saving the file being opened into the storage space, the automatic operation is either triggered by the application itself or the operating system.

37. (Canceled)

38. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 31, further comprising encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group of users.

39. (Currently Amended) The ~~computer readable storage~~ tangible computer-readable medium of Claim 31, further comprising attaching the header to the encrypted file, wherein the header includes the security information encrypted in addition to a flag indicating that the file is secured.

40. (Currently Amended) A computing device for securing a file, comprising:

an application configured to access the file that includes security information and an encrypted portion, the security information further including a file key and access rules, the encrypted portion being an encrypted version of the file; and

a cipher module configured to activate upon determining that the file being accessed is secured;

wherein the security information is configured to be encrypted with a user key, is configured to be decrypted with the user key when authenticated, and includes access rules of how and by whom the file is to be accessed; and

wherein the file key is configured to be retrieved to decrypt the encrypted portion only after the access rules have been successfully measured against access ~~privilege of a user.~~ privilege.

41. (Previously Presented) The computing device of Claim 40, further comprising an operating system configured to support operations of the application, and wherein the cipher module is embedded in the operating system.

42. (Previously Presented) The computing device of Claim 40, wherein the cipher module is configured to operate in a path through which the file is caused to pass when accessed by the application.

43. (Previously Presented) The computing device of Claim 40, further including a memory space and a storage space, and wherein the file key is temporarily kept in the memory space when the file is successfully loaded into the application.

44. (Previously Presented) The computing device of Claim 43, wherein the file key is deleted from the memory space as soon as the file is written back to the storage space.

45. (Currently Amended) The computing device of Claim 40, wherein the user key becomes authenticated ~~only when the user is authenticated~~ by an authentication process.

46. (Currently Amended) The computing device of Claim 40, wherein the computing device is coupled to a second computing device over a data network and the user key becomes authenticated only after ~~the user is successfully logged~~ successful logging from the computing device into the second computing device.

47. (Currently Amended) The computing device of Claim 40, wherein the computing device is provided with means for capturing biometric data ~~of the user~~ and the user key becomes authenticated only after the biometric data is successfully verified.

48. (Currently Amended) The computing device of Claim 40, wherein the user key becomes authenticated after the computing device receives credential ~~information from the user.~~ information.

49. (Currently Amended) The computing device of Claim 48, wherein the credential information includes at least one of a ~~password entered by the user,~~ password, biometric ~~information of the user, and~~ information, or personalized ~~information about the user.~~ information.

50. (Original) The computing device of Claim 49, wherein the biometric information is captured from a device coupled to the computing device.

51. (Previously Presented) The method of claim 1, further comprising:

launching the application when a request to access the file is received.

52. (Previously Presented) The method of claim 11, further comprising:

launching an application that accesses the file.

53. (Currently Amended) The method of claim 20, further comprising:

launching [[an]] the application under the operating system when the request to access the file is received.

54. (Currently Amended) The computer readable storage medium of claim 24, wherein the program code stored on the medium, when executed, causes [[an]] the application to be launched when a request to access the file is received.

55. (Previously Presented) The computer readable storage medium of claim 31, wherein the program code stored on the medium, when executed, causes the application to be launched.

56. (Previously Presented) The computing device of claim 40, wherein the application is launched to access the file.